EUROPESE COMMISSIE

HOGE VERTEGENWOORDIGER VAN DE EUROPESE UNIE VOOR BUITENLANDSE ZAKEN EN VEILIGHEIDSBELEID

Brussel, 7.2.2013
JOIN(2013) 1 final

GEZAMENLIJKE MEDEDELING AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Strategie inzake cyberbeveiliging van de Europese Unie:

Een open, veilige en beveiligde cyberspace

GEZAMENLIJKE MEDEDELING AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

Strategie inzake cyberbeveiliging van de Europese Unie:

Een open, veilige en beveiligde cyberspace

1. INLEIDING

1.1. Achtergrond

De laatste twintig jaar heeft het internet en ruimer gezien cyberspace een enorm effect op alle geledingen van de maatschappij gehad. Ons dagelijks leven, onze grondrechten, sociale interactie en economieën zijn ervan afhankelijk dat informatie- en communicatietechnologie soepel werkt. Open en vrije cyberspace heeft de politieke en maatschappelijke cohesie over de hele wereld bevorderd; het heeft obstakels tussen landen, gemeenschappen en burgers verwijderd alsmede interactie en het delen van informatie en ideeën over de hele wereld mogelijk gemaakt; het heeft een forum gecreëerd voor vrijheid van meningsuiting en het uitoefenen van grondrechten, en het heeft mensen in staat gesteld te streven naar democratische en rechtvaardigere samenlevingen – het meest in het oog springend tijdens de Arabische lente.

Om cyberspace open en vrij te houden, is het van belang dat de normen, beginselen en waarden die de EU erbuiten handhaaft ook in de digitale wereld worden toegepast. Grondrechten, democratie en de rechtsstaat dienen in cyberspace te worden beschermd. Onze vrijheid en welvaart hangen er in toenemende mate van af dat internet robuust en innovatief is; het blijft gedijen als de private sector en het maatschappelijk middenveld op basis van innovatie voor groei zorgen. Om vrijheid in de digitale wereld te waarborgen, is echter ook veiligheid en beveiliging nodig. Cyberspace moet worden beschermd tegen incidenten, kwaadwillige activiteiten en misbruik; overheden spelen een belangrijke rol bij het waarborgen van vrijheid en veiligheid in cyberspace. Overheden hebben diverse taken: het waarborgen van toegang en openheid, het respecteren en beschermen van grondrechten in de digitale wereld en het op peil houden van de betrouwbaarheid en interoperabiliteit van internet. De private sector bezit en exploiteert echter een aanzienlijk gedeelte van cyberspace. Initiatieven op dit gebied kunnen derhalve alleen slagen als het belang van de private sector wordt erkend.

Informatie- en communicatietechnologie is uitgegroeid tot de belangrijkste steunpilaar van economische groei en een kritische hulpbron waarvan alle economische sectoren afhankelijk zijn. Deze technologie vormt het fundament voor de complexe systemen die onze economieën draaiende houden in belangrijke sectoren zoals financiën, gezondheidszorg, energie en vervoer. Veel bedrijfsmodellen zijn erop gebaseerd dat internet zonder onderbreking beschikbaar is en dat informatiesystemen vlekkeloos werken.

Europa kan haar bbp door voltooiing van de digitale interne markt een impuls van bijna 500 miljard euro per jaar geven[1], dat is een gemiddelde van 1 000 euro per persoon. Om ervoor te zorgen dat nieuwe cyberspacetechnologieën aanslaan, met inbegrip van elektronisch betalen,

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

cloud computing en M2M-communicatie[2], moeten de burgers er vertrouwen in hebben. Uit een Eurobarometer-onderzoek van 2012[3] blijkt dat bijna eenderde van de Europeanen internet niet durft te gebruiken voor bankzaken of om iets te kopen. De overgrote meerderheid gaf daarnaast aan vanwege zorgen over de veiligheid op internet zo min mogelijk persoonlijke informatie vrij te geven. In de EU is al meer dan één op de tien internetgebruikers het slachtoffer geworden van internetfraude.

De laatste jaren is gebleken dat de digitale wereld enorme voordelen biedt, maar ook kwetsbaar is. Het aantal gerichte of onbedoelde incidenten op het gebied van de cyberbeveiliging[4] neemt schrikbarend snel toe. Dit zou kunnen leiden tot het uitvallen van essentiële diensten, zoals water, gezondheidszorg, elektriciteit of mobiele diensten, die wij vanzelfsprekend vinden. Dreigingen kunnen verschillende achtergronden hebben, zoals criminele, politiek gemotiveerde, terroristische of door een staat gesteunde aanvallen, alsmede natuurrampen en onbedoelde fouten.

De economie van de EU wordt al geconfronteerd met cybercriminaliteit[5] die is gericht tegen de private sector en individuen. De methoden die cybercriminelen gebruik om informatiesystemen binnen te dringen, kritieke gegevens te stelen of bedrijven af te persen, worden steeds geraffineerder. De toename van economische spionage en door staten gesteunde activiteiten in cyberspace vormt een nieuwe dreiging voor overheden en bedrijven in de EU.

In landen buiten de EU kunnen overheden cyberspace daarnaast misbruiken voor de bewaking van en controle over hun eigen burgers. De EU kan hieraan tegenstand bieden door vrijheid in de digitale wereld te bevorderen en te waarborgen dat de grondrechten in de digitale wereld worden gerespecteerd.

Al deze aspecten hebben ertoe geleid dat overheden over de hele wereld begonnen zijn strategieën op het gebied van cyberbeveiliging te ontwikkelen en cyberspace als steeds belangrijkere internationale kwestie zijn gaan beschouwen. Het is nu aan de EU om haar inspanningen op dit gebied te intensiveren. Dit voorstel voor een strategie inzake cyberbeveiliging van de Europese Unie dat is opgesteld door de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid, schetst de visie die de EU op dit gebied heeft, bakent rollen en verantwoordelijkheden af en omvat de vereiste maatregelen, op basis van een sterke en effectieve bescherming en bevordering van de rechten van de burgers, om de digitale omgeving in de EU de veiligste in de wereld te maken.

---

[2] Bijvoorbeeld sensoren die in planten zijn geïntegreerd en die zelf aan een bewateringssysteem doorgeven dat de planten water nodig hebben.

[3] Speciaal Eurobarometer-onderzoek 390 van 2012 over cyberbeveiliging.

[4] Cyberbeveiliging betekent over het algemeen de waarborgen en acties die kunnen worden toegepast om cyberspace te beschermen, zowel op burger- als op militair gebied, tegen dreigingen die gepaard gaan met of schade kunnen aanrichten aan onderling afhankelijke netwerken en de informatie-infrastructuur. Cyberbeveiliging is erop gericht de beschikbaarheid en integriteit van netwerken en infrastructuur in stand te houden, alsmede de vertrouwelijkheid van de informatie die zich daarin bevindt.

[5] Cybercriminaliteit betekent over het algemeen een breed bereik aan verschillende strafbare feiten waarbij computers en informatiesystemen zijn betrokken als primair middel of primair doelwit. Cybercriminaliteit omvat traditionele strafbare feiten (bijvoorbeeld fraude, vervalsing en identiteitsdiefstal), inhoudsgerelateerde misdrijven (bijvoorbeeld op internet beschikbaar stellen van kinderpornografie of aanzetten tot rassenhaat) en strafbare feiten die alleen in verband met computers en informatiesystemen worden gepleegd (bijvoorbeeld aanvallen tegen informatiesystemen, denial-of-service-aanvallen en malware oftewel kwaadaardige software).

1.2. Beginselen inzake cyberbeveiliging

Het grensoverschrijdende en gelaagde internet is uitgegroeid tot een van de sterkste motoren voor vooruitgang op wereldwijde schaal waarop overheden geen toezicht of regelgeving toepassen. De private sector moet een vooraanstaande rol blijven spelen bij de constructie en het dagelijks beheer van internet, maar de behoefte aan vereisten voor transparantie, controleerbaarheid en beveiliging wordt steeds groter. Deze strategie omvat uitleg over de beginselen waarop het cyberbeveiligingsbeleid in de EU en op internationaal niveau dient te worden gebaseerd.

De kernwaarden van de EU gelden net zo goed voor de digitale als voor de fysieke wereld

De wetten en normen die van toepassing zijn op andere aspecten van ons dagelijks leven gelden ook voor cyberspace.

Bescherming van grondrechten, de vrijheid van meningsuiting, persoonsgegevens en de persoonlijke levenssfeer

Cyberbeveiliging kan alleen en krachtig en doeltreffend zijn als het is gebaseerd op de grondrechten en vrijheden als vastgelegd in het Handvest van de grondrechten van de Europese Unie en de kernwaarden van de EU. De rechten van het individu kunnen op hun beurt niet worden beschermd zonder veilige netwerken en systemen. Elke vorm van delen van informatie ten bate van cyberbeveiliging waarbij gebruik wordt gemaakt van persoonsgegevens dient in overeenstemming te zijn met de gegevensbeschermingswetgeving van de EU. Daarnaast dienen hierbij de rechten van het individu op dit gebied volledig te worden geëerbiedigd.

Toegang voor iedereen

Door beperkte of ontbrekende toegang tot internet en door digitaal analfabetisme worden burgers benadeeld, aangezien de digitale wereld in alle geledingen van de maatschappij is doorgedrongen. Iedereen dient toegang tot internet en een ongehinderde stroom van informatie te hebben. De integriteit en beveiliging van internet dient te zijn gewaarborgd, zodat iedereen op een veilige manier toegang heeft.

Democratische en efficiënte multistakeholder-governance

De digitale wereld wordt niet door één enkele instantie bestuurd. Er zijn diverse belanghebbende partijen, waaronder vele commerciële en niet-gouvernementele entiteiten, betrokken bij het dagelijks beheer van internetvoorzieningen, -protocollen en -normen en bij de toekomstige ontwikkeling van internet. De EU bevestigt het belang van alle belanghebbende partijen voor het huidige internetgovernancemodel en steunt de aanpak op basis van multistakeholder-governance[6].

Gedeelde verantwoordelijkheid voor beveiliging

De toenemende afhankelijkheid van informatie- en communicatietechnologieën op alle gebieden van het leven heeft geleid tot een aantal zwakke plekken, die naar behoren dienen te worden bepaald, geanalyseerd, weggewerkt dan wel teruggedrongen. Of het overheden, de

[6] Zie ook COM(2009) 277, Mededeling van de Commissie aan het Europees Parlement en de Raad inzake "Internetgovernance: de volgende stappen".

private sector of individuele burgers zijn: alle betrokkenen dienen deze gedeelde verantwoordelijkheid te erkennen, maatregelen te nemen om zichzelf te beschermen en zo nodig te zorgen voor een gecoördineerde reactie om de cyberbeveiliging te versterken.

2. STRATEGISCHE PRIORITEITEN EN MAATREGELEN

De EU dient waarborgen te bieden voor een digitale omgeving met een zo hoog mogelijk niveau van vrijheid en beveiliging ten bate van iedereen. Bij deze strategie wordt enerzijds erkend dat de verantwoordelijkheid voor het aanpakken van beveiligingsproblemen in cyberspace voornamelijk bij de lidstaten ligt en worden anderzijds specifieke maatregelen voorgesteld die ertoe kunnen leiden dat de EU als geheel op dit gebied beter presteert. Dit zijn zowel langetermijn- als kortetermijnmaatregelen die uiteenlopende beleidsinstrumenten omvatten[7] en waarbij verschillende partijen betrokken zijn, waaronder EU-instellingen, de lidstaten en de sector.

De EU-visie die in het kader van deze strategie wordt gepresenteerd, omvat vijf strategische prioriteiten die betrekking hebben op de hierboven vermelde kwesties:

- cyberspace veerkrachtig maken;
- cybercriminaliteit drastisch terugdringen;
- cyberdefensiebeleid- en capaciteit ontwikkelen in het kader van het gemeenschappelijke veiligheids- en defensiebeleid (GVDB);
- de industriële en technologische voorzieningen voor cyberbeveiliging ontwikkelen;
- een coherent internationaal cyberbeveiligingsbeleid voor de Europese Unie ontwikkelen en de kernwaarden van de EU uitdragen.

2.1. Cyberspace veerkrachtig maken

Om de veerkracht van cyberspace in de EU te bevorderen, moeten zowel de overheden als de private sector capaciteit ontwikkelen en doeltreffend samenwerken. Verdere actie door de EU kan worden gebaseerd op de activiteiten die tot nu zijn verricht[8]. Dit is met name nuttig bij het aanpakken van cyberrisico's en -dreigingen van grensoverschrijdende aard en kan bijdragen tot een gecoördineerde reactie op noodsituaties. Dit zal zeer bevorderlijk zijn voor de goede werking van de interne markt en de interne beveiliging in de EU verbeteren.

Als er geen uitgebreide maatregelen worden genomen om de publieke en private capaciteit, voorzieningen en processen te versterken die zijn gericht op het voorkomen, opsporen en aanpakken van incidenten op het vlak van cyberbeveiliging, zal Europa kwetsbaar blijven. Om die reden heeft de Commissie beleid inzake netwerk- en informatiebeveiliging (NIB) ontwikkeld[9]. In 2004 werd het **Europees Agentschap voor netwerk- en**

[7] De maatregelen met betrekking tot het delen van informatie waarbij gebruik wordt gemaakt van persoonsgegevens dient in overeenstemming te zijn met de gegevensbeschermingswetgeving van de EU.

[8] Zie verwijzingen in deze mededeling en in het werkdocument van de diensten van de Commissie "Effectbeoordeling, gevoegd bij het Commissievoorstel voor een richtlijn inzake netwerk- en informatiebeveiliging", met name de hoofdstukken 4.1.4 en 5.2 alsmede bijlage 2, bijlage 6 en bijlage 8.

[9] In 2001 heeft de Commissie een mededeling aangenomen over "Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak" (COM(2001) 298); in 2006 heeft zij een strategie voor een veilige informatiemaatschappij aangenomen (COM(2006) 251). Vanaf 2009 heeft de Commissie verder een actieplan en een mededeling aangenomen betreffende de bescherming van kritieke informatie-infrastructuur (COM(2009) 149, zoals goedgekeurd door de resolutie 2009/C 321/01 van de Raad alsmede COM(2011) 163, zoals bekrachtigd door de conclusies 10299/11 van de Raad).

informatiebeveiliging (ENISA) opgericht[10] en momenteel onderhandelen de Raad en het Europees Parlement over een nieuwe verordening inzake de versterking van ENISA en de modernisering van het mandaat van dit agentschap[11]. Daarnaast stelt de Kaderrichtlijn voor elektronische-communicatienetwerken en -diensten[12] leveranciers van elektronische-communicatiediensten verplicht om de risico's voor de veiligheid van hun netwerken goed te beheersen en om ernstige inbreuken op de veiligheid te melden. Bovendien stelt de gegevensbeschermingswetgeving van de EU[13] degenen die verantwoordelijk zijn voor de verwerking van gegevens verplicht om vereisten en waarborgen ten aanzien van de gegevensbescherming vast te leggen, met inbegrip van maatregelen betreffende de beveiliging; bij openbare elektronische-communicatiediensten moeten zij inbreuken in verband met persoonsgegevens melden aan de bevoegde nationale instanties.

Op basis van vrijwillige verplichtingen is er wel vooruitgang geboekt, maar in de EU zijn er nog steeds lacunes, met name op het gebied van nationale capaciteit, coördinatie bij grensoverschrijdende incidenten en de betrokkenheid en paraatheid van de private sector. De strategie wordt vergezeld door een **wetgevingsvoorstel** dat met name op het volgende is gericht:

- het vastleggen van gemeenschappelijk minimumeisen voor NIB op nationaal niveau om de lidstaten verplicht te stellen om: nationale instanties aan te wijzen die voor NIB bevoegd zijn; een goed functionerend CERT (computercrisisteam) op te richten; en een nationale strategie alsmede een nationaal samenwerkingsplan inzake NIB vast te stellen. Bij het opbouwen en de coördinatie van capaciteit zijn ook de EU-instellingen betrokken: in 2012 werd er een permanent computercrisisteam ("CERT-EU") opgericht, dat verantwoordelijk is voor de beveiliging van de IT-systemen van de EU-instellingen, -agentschappen en -organen;
- het instellen van gecoördineerde mechanismen voor de preventie, opsporing, schadebeperking en reactie, die het de voor NIB bevoegde nationale instanties mogelijk maken informatie te delen en wederzijdse bijstand te verlenen. Van de voor netwerk- en informatiebeveiliging bevoegde nationale instanties wordt gevraagd op EU-niveau naar behoren met elkaar samen te werken, met name op basis van een samenwerkingsplan inzake NIB van de Unie dat erop is gericht te reageren op grensoverschrijdende cyberincidenten. Deze samenwerking zal voortbouwen op de vooruitgang die is geboekt in het kader van het "Europees Forum voor de lidstaten"[14], waarbinnen productief overleg is gepleegd betreffende overheidsbeleid inzake NIB; dit kan worden geïntegreerd in het samenwerkingsmechanisme, zodra dat is ingesteld;
- het verbeteren van de paraatheid en de betrokkenheid van de private sector. Aangezien het overgrote deel van de netwerk- en informatiesystemen eigendom is van de private sector en door deze sector wordt geëxploiteerd, is het van essentieel belang dat de private sector meer wordt betrokken bij het bevorderen van cyberbeveiliging. De private sector dient eigen technische capaciteit op het gebied van de veerkracht van cyberspace te ontwikkelen en beste praktijken binnen alle branches te delen. De instrumenten die de private sector ontwikkelt om op incidenten te reageren, de oorzaken daarvan te bepalen en forensisch

[10] Verordening (EU) nr. 460/2004.
[11] COM(2010) 521. De maatregelen die in het kader van deze strategie worden voorgesteld, houden geen wijziging in van het bestaande of toekomstige mandaat van het ENISA.
[12] Artikel 13 bis en ter van Richtlijn 2002/21/EG.
[13] Artikel 17 van Richtlijn 95/46/EG; artikel 4 van Richtlijn 2002/58/EG.
[14] Het Europees Forum voor de lidstaten is gelanceerd bij COM(2009) 149 als platform om overleg tussen de overheden van de lidstaten te bevorderen met betrekking tot goede beleidspraktijken op het gebied van de beveiliging en veerkracht van kritieke informatie-infrastructuur.

onderzoek te doen, moeten ook ten bate van de publieke sector beschikbaar worden gesteld.

De private actoren worden echter niet genoeg aangemoedigd om betrouwbare gegevens over het optreden of de gevolgen van NIB-incidenten ter beschikking te stellen, een risicobeheerscultuur te ontwikkelen of in beveiligingsoplossingen te investeren. De voorgestelde wetgeving is er daarom op gericht ervoor te zorgen dat de spelers op een aantal essentiële gebieden (namelijk energie, vervoer, banken, effectenbeurzen, facilitatoren van essentiële internetdiensten en overheden) evalueren met welke dreigingen voor de cyberbeveiliging zij worden geconfronteerd, dat zij door middel van afdoende risicobeheersmaatregelen waarborgen dat netwerken en informatiesystemen betrouwbaar en veerkrachtig zijn en dat zij informatie daarover ter beschikking stellen aan de nationale instanties die voor NIB bevoegd zijn. Als er een cyberbeveiligingscultuur wordt ingevoerd, biedt dat zakelijke mogelijkheden en een betere concurrentiepositie voor de private sector. Cyberbeveiliging zou dan een verkoopargument zijn.

De bovengenoemde spelers zouden aan de voor NIB bevoegde nationale instanties melding moeten maken van incidenten met een aanzienlijke impact voor de continuïteit van de belangrijkste diensten en de levering van goederen, waarvoor netwerk- en informatiesystemen nodig zijn.

De nationale instanties die voor NIS bevoegd zijn, dienen samen te werken en informatie uit te wisselen met andere toezichthoudende instanties, en met name met de gegevensbeschermingsautoriteiten. De voor NIB bevoegde nationale instanties dienen op hun beurt melding van incidenten van vermoedelijk ernstig criminele aard te maken aan de wetshandhavingsinstanties. De bevoegde nationale instanties dienen daarnaast regelmatig niet-vertrouwelijke informatie over actuele vroegtijdige waarschuwingen voor incidenten en risico's alsmede over gecoördineerde reacties bekend te maken op een speciale website. Wettelijke verplichtingen mogen geen vervanging of belemmering vormen voor het ontwikkelen van informele en vrijwillige samenwerking, met inbegrip van samenwerking tussen de publieke en de private sector, met het oog op de verhoging van beveiligingsniveaus en de uitwisseling van informatie en beste praktijken. Met name het Europees publiek-privaat partnerschap voor veerkracht (EP3R[15]) is op EU-niveau een stevig en deugdelijk platform dat verder ontwikkeld dient te worden.

Essentiële infrastructuur kan financiële steun krijgen uit de financieringsfaciliteit voor Europese verbindingen (CEF)[16], waarbij de capaciteit van de lidstaten op het gebied van NIB wordt gekoppeld en samenwerking in de hele EU wordt vergemakkelijkt.

Tot slot zijn oefeningen met betrekking tot cyberincidenten op EU-niveau essentieel om de samenwerking tussen de lidstaten en de private sector te bevorderen. De eerste oefening waarbij lidstaten waren betrokken, vond plaats in 2010 ("Cyber Europe 2010") en een tweede oefening, waarbij ook de private sector was betrokken, in oktober 2012 ("Cyber Europe 2012"). Een gezamenlijke simulatie-oefening van de EU en de Verenigde Staten vond plaats

15 Het Europees publiek-privaat partnerschap voor veerkracht is ingesteld naar aanleiding van COM(2009) 149. Dit platform heeft initiatieven ontwikkeld en de samenwerking tussen de publieke en de private sector bevorderd met betrekking tot het bepalen van essentiële elementen, voorzieningen, functies, basisvereisten op het gebied van veerkracht alsmede vereiste samenwerking en mechanismen ter bestrijding van grootschalige verstoringen van de elektronische communicatie.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. CEF-begrotingsonderdeel 09.03.02 – Telecommunicatienetwerken (ter bevordering van de onderlinge koppeling en interoperabiliteit van nationale openbare onlinediensten en van de toegang tot dergelijke netwerken).

in november 2011 ("Cyber Atlantic 2011"). Voor de komende jaren zijn er nog meer oefeningen gepland, onder meer met internationale partners.

De Commissie zal de volgende stappen ondernemen:

- de activiteiten voortzetten die door het Gemeenschappelijk Centrum voor Onderzoek in nauw overleg met de instanties van de lidstaten alsmede de eigenaars en exploitanten van kritieke infrastructuur worden verricht om zwakke plekken in de NIB van kritieke infrastructuur in Europa te bepalen en de ontwikkeling van veerkrachtige systemen aan te moedigen;
- begin 2013 een door de EU gefinancierd proefproject[17] lanceren op het gebied van de bestrijding van **botnets en malware** om een kader te bieden voor overleg en samenwerking tussen de EU-lidstaten, organisaties uit de private sector, met inbegrip van internetaanbieders, en internationale partners.

De Commissie vraagt ENISA het volgende:

- de lidstaten te helpen om een solide **nationale capaciteit te ontwikkelen om cyberspace veerkrachtig te maken**, met name door het opbouwen van expertise over de beveiliging en veerkracht van industriële besturingssystemen, het vervoer en de energie-infrastructuur;
- in 2013 de haalbaarheid te bestuderen van één of meer computercrisisteams voor industriële besturingssystemen (ICS-CSIRT's) voor de EU;
- zijn steun aan de lidstaten en de EU-instellingen voort te zetten door regelmatig **pan-Europese oefeningen met betrekking tot cyberincidenten** uit te voeren, die tevens de operationele basis vormen voor deelname van de EU aan internationale oefeningen met betrekking tot cyberincidenten.

De Commissie verzoekt het Europees Parlement en de Raad om het volgende:

- het voorstel voor een richtlijn inzake een **gemeenschappelijk hoog niveau van netwerk- en informatiebeveiliging (NIB)** in de EU spoedig **vast te stellen**, met het oog op nationale capaciteit en paraatheid, samenwerking op EU-niveau, de invoering van risicobeheerspraktijken en het delen van informatie over netwerk- en informatiebeveiliging.

De Commissie vraagt de sector om het volgende:

- het initiatief te nemen bij het **investeren** in een hoog niveau van cyberbeveiliging, beste praktijken te ontwikkelen en informatie te delen op sectorniveau en met overheden met het oog op het waarborgen van een sterke en doeltreffende bescherming van voorzieningen en individuen, met name door middel van publiek-private partnerschappen, zoals EP3R en Trust in Digital Life (TDL)[18].
-

[17] CIP-ICT PSP-2012-6, 325188. Dit project beschikt over een totaalbudget van 15 miljoen euro, waarvan 7,7 miljoen euro EU-financiering.

[18] http://www.trustindigitallife.eu

Bewustmaking

Het waarborgen van cyberbeveiliging is een gemeenschappelijke verantwoordelijkheid. Eindgebruikers spelen een cruciale rol bij het waarborgen van de beveiliging van netwerken en informatiesystemen: zij dienen zich bewust te zijn van de risico's die zij in de digitale wereld lopen en de mogelijkheid te krijgen eenvoudige maatregelen te nemen om zich daartegen te beschermen.

De afgelopen jaren zijn er diverse initiatieven ontplooid die voortgezet dienen te worden. Zo was ENISA betrokken bij bewustmaking door verslagen te publiceren, workshops met deskundigen te organiseren en publiek-private partnerschappen te ontwikkelen. Ook Europol, Eurojust en nationale gegevensbeschermingsautoriteiten zijn op dit gebied actief. In oktober 2012 heeft ENISA samen met een aantal lidstaten het initiatief voor de "Europese maand van de cyberbeveiliging" genomen. Bewustmaking is een van de zwaartepunten van de gezamenlijke werkgroep voor cyberbeveiliging en cybercriminaliteit van de EU en de Verenigde Staten[19] en is ook essentieel in het kader van het Programma veiliger internet[20], dat gericht is op digitale veiligheid voor kinderen.

[19] Deze werkgroep is opgericht tijdens EU-Amerikaanse top van november 2010 (MEMO/10/597) en is belast met het ontwikkelen van een gezamenlijke aanpak voor een brede waaier aan problemen op het gebied van cyberbeveiliging en -criminaliteit.

[20] Met het "Programma veiliger internet" wordt een netwerk van NGO's gefinancierd die actief zijn op het gebied van digitaal welzijn van kinderen alsmede een netwerk van wetshandhavingsinstanties die informatie en beste praktijken uitwisselen betreffende crimineel gebruik van het internet voor het verspreiden van materiaal waarin kinderen seksueel misbruikt worden en een netwerk van onderzoekers die informatie verzamelen over het gebruik, de risico's en de gevolgen van onlinetechnologieën met betrekking tot het leven van kinderen.

De Commissie vraagt ENISA het volgende:

- in 2013 een stappenplan voor te stellen voor een "rijbewijs voor netwerk- en informatiebeveiliging" in het kader van een facultatief certificeringsprogramma om gevorderde vaardigheden en kennis van IT-specialisten (bijvoorbeeld websitebeheerders) te bevorderen.

De Commissie zal de volgende stappen ondernemen:

- in 2014 met steun van ENISA een **kampioenschap** cyberbeveiliging organiseren, waarbij universiteitsstudenten het tegen elkaar opnemen met oplossingen op het gebied van NIB die zij hebben ontwikkeld.

De Commissie verzoekt de lidstaten[21] om het volgende:

- jaarlijks met steun van ENISA en in overleg met de private sector vanaf 2013 een **maand van de cyberbeveiliging** te organiseren met het doel de eindgebruikers bewuster te maken. Te beginnen in 2014 wordt de maand van de cyberbeveiliging tegelijkertijd in de EU en de Verenigde Staten georganiseerd;
- **meer werk te maken van opleidingen en cursussen betreffende NIB** door het volgende in te voeren: lessen over NIB op scholen tegen 2014; cursussen over NIB, ontwikkeling van veilige software en bescherming van persoonsgegevens voor informaticastudenten; en basiscursussen NIB voor personeel van overheidsdiensten.

De Commissie verzoekt de sector het volgende:

- **bewustmaking** inzake cyberbeveiliging **op alle niveaus** te bevorderen, zowel in de praktijk van het bedrijfsleven als in contacten met klanten. Met name dient de sector te overwegen op welke manier CEO's en raden van bestuur meer verantwoording kunnen afleggen voor het waarborgen van cyberbeveiliging.

2.2. Cybercriminaliteit drastisch terugdringen

De digitale wereld wordt steeds uitgebreider, waardoor cybercriminelen steeds meer kansen krijgen. Cybercriminaliteit is een van de snelstgroeiende vormen van criminaliteit: elke dag zijn er wereldwijd meer dan één miljoen mensen per wereld slachtoffer van. Cybercriminelen en cybercriminaliteitsnetwerken worden steeds geraffineerder. Dit kan alleen met de juiste operationele middelen en capaciteit worden aangepakt. Cybercriminaliteit is zeer winstgevend en de pakkans is klein. Criminelen maken vaak misbruik van de anonimiteit die websites bieden. Cybercriminaliteit wordt niet door grenzen tegengehouden: het wereldwijde bereik van het internet houdt in dat de wetshandhaving deze toenemende dreiging alleen kan aanpakken door middel van een gecoördineerde en gezamenlijke benadering.

Sterke en effectieve wetgeving

De EU en de lidstaten hebben sterke en effectieve wetgeving nodig om cybercriminaliteit aan te pakken. Het Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten

[21] Met inbegrip van de desbetreffende nationale autoriteiten, waaronder de voor netwerk- en informatiebeveiliging bevoegde instanties en de gegevensbeschermingsautoriteiten.

verbonden met elektronische netwerken, ook bekend als het Verdrag van Boedapest, is een bindend internationaal verdrag dat een effectief kader biedt voor de vaststelling van nationale wetgeving.

De EU heeft al wetgeving inzake cybercriminaliteit vastgesteld, met inbegrip van een richtlijn ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie[22]. De EU heeft ook nagenoeg overeenstemming bereikt over een richtlijn inzake aanvallen op informatiesystemen, met name met gebruikmaking van botnets.

De Commissie zal de volgende stappen ondernemen:

- zorgen voor spoedige omzetting en tenuitvoerlegging van de richtlijnen op het gebied van cybercriminaliteit;
- de lidstaten die het **Verdrag van de Raad van Europa inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken** nog niet hebben bekrachtigd, aansporen dit verdrag zo spoedig mogelijk te bekrachtigen en ten uitvoer te leggen.

Verbeterde operationele capaciteit om cybercriminaliteit te bestrijden

De technieken waarvan in de cybercriminaliteit gebruikt wordt gemaakt, ontwikkelen zich steeds sneller. Wetshandhavingsinstanties kunnen cybercriminaliteit niet bestrijden met achterhaalde operationele middelen. Momenteel beschikken niet alle EU-lidstaten over de operationele capaciteit die nodig is om cybercriminaliteit doeltreffend aan te pakken. Alle lidstaten hebben effectieve nationale diensten voor de bestrijding van cybercriminaliteit nodig.

De Commissie zal de volgende stappen ondernemen:

- de lidstaten via financieringsprogramma's[23] ondersteunen om **lacunes te bepalen en hun capaciteit te vergroten** met betrekking tot onderzoek naar en bestrijding van cybercriminaliteit. De Commissie zal bovendien instanties ondersteunen die de koppeling maken tussen wetenschappelijk onderzoek/de academische wereld, rechtshandhavingsinstanties en de private sector, zoals momenteel in de praktijk wordt gebracht door de kenniscentra op het gebied van cybercriminaliteit die in een aantal landen zijn opgezet en die worden gefinancierd door de Commissie;
- samen met de lidstaten ervoor zorgen dat de beste praktijken en beste beschikbare technieken ter bestrijding van cybercriminaliteit op een gecoördineerde manier worden bepaald, waarbij het Gemeenschappelijk Centrum voor Onderzoek wordt betrokken (bijvoorbeeld met betrekking tot de ontwikkeling en het gebruik van forensische middelen of dreigingsanalyse);
- nauw samenwerken met het onlangs opgerichte **Europees Centrum voor de bestrijding van cybercriminaliteit (EC3), met Europol en met Eurojust** om dergelijke beleidsbenaderingen af te stemmen op beste praktijken aan de

[22] Richtlijn 2011/93/EU ter vervanging van Kaderbesluit 2004/68/JHA van de Raad.

[23] Voor 2013 op grond van het programma Preventie en bestrijding van criminaliteit (ISEC). Na 2013 op grond van het fonds voor interne veiligheid (nieuw instrument binnen het meerjarig financieel kader).

operationele zijde.

Verbeterde coördinatie op EU-niveau

De EU kan het werk van de lidstaten aanvullen door een gecoördineerde en gezamenlijke aanpak te bevorderen, en wetshandhavingsinstanties, gerechtelijke autoriteiten alsmede publieke en private belanghebbende partijen van binnen en buiten de EU samen te brengen.

De Commissie zal de volgende stappen ondernemen:

- het onlangs opgerichte **Europees Centrum voor de bestrijding van cybercriminaliteit** (EC3) ondersteunen als Europees spil voor de bestrijding van cybercriminaliteit. Het EC3 verstrekt analyses en inlichtingen, steunt onderzoek, biedt hoogwaardige forensische diensten, bevordert samenwerking, schept kanalen voor het delen van informatie tussen de bevoegde autoriteiten in de lidstaten, de private sector en andere belanghebbende partijen, en zal op den duur fungeren als spreekbuis voor de rechtshandhavingsgemeenschap[24];
- inspanningen ondersteunen om de controleerbaarheid van domeinnaamregistrars te verhogen en de nauwkeurigheid te waarborgen van informatie over de eigenaren van websites, met name op basis van de rechtshandhavingsaanbevelingen voor de Internet Corporation for Assigned Names and Numbers (ICANN), overeenkomstig de Unie-wetgeving, met inbegrip van de regels inzake gegevensbescherming;
- voortbouwen op recente wetgeving om de inspanningen van de EU ter bestrijding van seksuele uitbuiting van kinderen via het internet te versterken. De Commissie heeft een Europese strategie voor een beter internet voor kinderen[25] aangenomen en samen met EU- en niet-EU-landen een **Wereldwijde alliantie tegen seksuele uitbuiting van kinderen via het internet**[26] opgezet. De alliantie is een door de Commissie en EC3 gesteund platform op basis waarvan de lidstaten verdere maatregelen kunnen ontplooien.

De Commissie vraagt Europol (EC3) om:

- haar analytische en operationele steun hoofdzakelijk te richten op onderzoek dat de lidstaten naar cybercriminaliteit doen, om in eerste instantie voornamelijk te helpen cybercriminaliteitsnetwerken op het gebied van seksuele uitbuiting van kinderen, betalingsfraude, botnets en binnendringing aan te pakken;
- regelmatig strategische en operationele verslagen uit te brengen over trends en opkomende dreigingen met het oog op het bepalen van prioriteiten en het uitvoeren van onderzoek door cybercriminaliteitbestrijdingsteams in de lidstaten.

---

[24] Op 28 maart 2012 heeft de Europese Commissie een mededeling met de titel "De aanpak van criminaliteit in het digitale tijdperk – Oprichting van een Europees Centrum voor de bestrijding van cybercriminaliteit" goedgekeurd.

[25] COM(2012) 196 final.

[26] Conclusies van de Raad over een Wereldwijde alliantie tegen seksuele uitbuiting van kinderen via het internet (gezamenlijke verklaring EU-VS) 7 en 8 juni 2012 en Verklaring over de start van de Wereldwijde alliantie tegen seksuele uitbuiting van kinderen via het internet (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)

De Commissie vraag de Europese Politieacademie (CEPOL) om samen met Europol de volgende stappen te ondernemen:

- cursussen te ontwikkelen en te organiseren om de wetshandhavingsinstanties te voorzien van de kennis en expertise die nodig is om cybercriminaliteit doeltreffend aan te pakken.

De Commissie vraagt Eurojust om de volgende stappen te ondernemen:

- aan te geven wat de belangrijkste hinderpalen voor justitiële samenwerking op het gebied van onderzoek naar cybercriminaliteit en voor overleg tussen de lidstaten onderling en met betrekking tot derde landen zijn, en op operationeel en strategisch vlak steun te geven aan het onderzoek naar en de vervolging van cybercriminaliteit alsmede aan trainingsactiviteiten in de praktijk.

De Commissie vraagt Eurojust en Europol (EC3) om de volgende stappen te ondernemen:

- nauw samen te werken, onder meer door informatie uit te wisselen, teneinde overeenkomstig hun respectievelijke mandaten en bevoegdheden hun effectiviteit bij de bestrijding van cybercriminaliteit te verhogen.

2.3. Cyberdefensiebeleid- en capaciteit ontwikkelen in het kader van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB)

Bij inspanningen in de EU op het gebied van cyberbeveiliging dient ook rekening te worden gehouden met de dimensie cyberdefensie. Om de veerkracht te verhogen van de communicatie- en informatiesystemen die de belangen van de lidstaten op het gebied van defensie en nationale veiligheid ondersteunen, dient de cyberdefensiecapaciteit met name met betrekking tot opsporing, bestrijding en herstel inzake geraffineerde cyberdreigingen te worden ontwikkeld.

Aangezien deze dreigingen veel aspecten hebben, dient de synergie tussen de civiele en militaire benadering ter bescherming van kritieke cybervoorzieningen te worden verbeterd. Deze inspanningen dienen te worden gesteund door onderzoek en ontwikkeling en door nauwere samenwerking tussen overheden, de private sector en de academische wereld in de EU. Om dubbel werk te vermijden, zal de EU nagaan hoe de EU en de NAVO de handen ineen kunnen slaan om de veerkracht te verhogen van kritieke informatie-infrastructuur op het gebied van onder meer overheden en defensie, waarvan de leden van beide organisaties afhankelijk zijn.

De hoge vertegenwoordiger zal zich richten op de volgende belangrijke activiteiten en de lidstaten en het Europees Defensieagentschap vragen met elkaar samen te werken:

- evalueren wat de operationele vereisten van de EU op het gebied van cyberdefensie zijn, de ontwikkeling van de capaciteit en technologieën van de EU op het gebied van cyberdefensie bevorderen, waarbij alle aspecten van de ontwikkeling van capaciteit dienen te worden betrokken, met inbegrip van beginselen, leiderschap, organisatie, personeel, training, technologie, infrastructuur, logistiek en interoperabiliteit;

- het EU-beleidskader inzake cyberdefensie ontwikkelen om netwerken te beschermen die zijn betrokken bij GVDB-missies en -operaties, met inbegrip van dynamisch risicobeheer, verbeterde dreigingsanalyse en delen van informatie. Verbeteren van de mogelijkheden tot training en oefeningen inzake cyberdefensie voor de strijdkrachten op Europees en multinationaal vlak, met inbegrip van de integratie van cyberdefensie-elementen in bestaande oefeningsprogramma's;

- de dialoog en het overleg tussen civiele en militaire betrokkenen in de EU bevorderen, met nadruk op het uitwisselen van goede praktijken, informatie en vroegtijdige waarschuwingen, respons bij incidenten, risicoanalyse, bewustmaking en het vastleggen van cyberbeveiliging als prioriteit;

- zorgen voor een dialoog met internationale partners, met inbegrip van de NAVO, andere internationale organisaties en multinationale kenniscentra, met het oog op effectieve defensiecapaciteit, het bepalen van gebieden waarop samenwerking nuttig is en het vermijden van dubbel werk.

2.4. De industriële en technologische voorzieningen voor cyberbeveiliging ontwikkelen

Europa beschikt over hoogwaardige capaciteit met betrekking tot onderzoek en ontwikkeling, maar veel wereldwijd vooraanstaande aanbieders van innovatieve ICT-producten en -diensten zijn buiten de EU gevestigd. Het risico bestaat dat Europa niet alleen te afhankelijk wordt van ICT die elders wordt vervaardigd, maar ook van beveiligingsoplossingen die buiten haar grenzen worden ontwikkeld. Het is daarom van essentieel belang dat in de EU en in derde landen geproduceerde hardware- en softwarecomponenten die worden gebruikt in kritieke diensten en infrastructuur, alsmede in toenemende mate in mobiele apparaten, betrouwbaar en veilig zijn en dat deze waarborgen dat persoonsgegevens worden beschermd.

Bevorderen van een eengemaakte markt voor cyberbeveiligingsproducten

Een hoog beveiligingsniveau kan alleen worden gewaarborgd als de beveiliging voor alle betrokkenen binnen de waardeketen (bijvoorbeeld fabrikanten van apparatuur, softwareontwikkelaars, dienstverlener van de informatiemaatschappij) een prioriteit is. Veel betrokkenen beschouwen beveiliging blijkbaar nog steeds als extra last; er is weinig vraag naar beveiligingsoplossingen[27]. Er dienen passende prestatievereisten inzake cyberbeveiliging te worden opgesteld die binnen de hele waardeketen gelden voor in Europa toegepaste ICT-producten. De private sector moet worden aangemoedigd een hoog niveau van cyberbeveiliging te waarborgen. Als er labels worden ingevoerd die een adequate cyberbeveiligingsprestatie aangeven, kunnen bedrijven met goede cyberbeveiligingsprestatie en staat van dienst dit als verkoopargument gebruiken en daardoor van een concurrentievoordeel profiteren. De verplichtingen die de voorgestelde richtlijn inzake netwerk- en informatiebeveiliging oplegt, zouden bovendien een aanzienlijke impuls geven aan de concurrentie in de betrokken sectoren.

Daarnaast moet de Europese marktvraag naar producten met een zeer hoog beveiligingsniveau worden bevorderd. De strategie is er ten eerste op gericht de samenwerking en transparantie op het gebied van de beveiliging van ICT-producten te verbeteren. Daartoe dient er een platform te worden opgezet, waarop de desbetreffende Europese publieke en private

[27] Zie het werkdocument van de diensten van de Commissie (effectbeoordeling) bij het voorstel van de Commissie voor een richtlijn inzake netwerk- en informatiebeveiliging, hoofdstuk 4.1.5.2.

belanghebbende partijen samenkomen om goede praktijken op het gebied van de hele waardeketen van cyberbeveiliging vast te stellen en gunstige marktvoorwaarden te creëren voor de ontwikkeling en implementatie van veilige ICT-oplossingen. Een van de voornaamste maatregelen is het creëren van prikkels om passend risicobeheer toe te passen, beveiligingsnormen en -oplossingen aan te nemen alsmede eventueel facultatieve EU-brede certificeringsregelingen vast te leggen, die voortbouwen op bestaande regelingen uit de EU en derde landen. De Commissie zal bevorderen dat de lidstaten coherente benaderingen vaststellen om onevenwichtigheden te voorkomen die ertoe kunnen leiden dat bedrijven op grond van hun vestigingsplaats worden benadeeld.

Daarnaast zal de Commissie de ontwikkeling van beveiligingsnormen steunen en bijstand bieden op het vlak van EU-brede facultatieve certificeringsregelingen voor cloud computing, waarbij naar behoren rekening wordt gehouden met de noodzaak voor gegevensbescherming. De nadruk dient op de beveiliging van de productieketen te worden gelegd, met name voor essentiële economische sectoren (industriële besturingssystemen, energie- en vervoersinfrastructuur). Daarbij dient te worden voortgebouwd op het werk dat momenteel wordt verricht door de Europese normalisatieorganisaties (CEN, CENELEC en ETSI)[28] en de Cybersecurity Coordination Group (CSCG) alsmede op de expertise van ENISA, de Commissie en andere relevante betrokkenen.

De Commissie zal de volgende stappen ondernemen:

- in 2013 een publiek-privaat **platform inzake oplossingen op het gebied van NIB** oprichten om prikkels voor de implementatie van veilige ICT-oplossingen en de acceptatie van goede prestaties op het gebied van cyberbeveiliging toe te passen op ICT-producten die in Europa worden gebruikt;
- in 2014 aanbevelingen doen om cyberbeveiliging in de hele ICT-waardeketen te waarborgen, waarbij wordt voortgebouwd op het werk dat in het kader van het platform wordt verricht;
- onderzoeken hoe de belangrijkste aanbieders van ICT-hardware en -software de nationale bevoegde autoriteiten kunnen inlichten over opgespoorde zwakke plekken die de beveiliging aanzienlijk in het gedrang zouden kunnen brengen.

De Commissie vraagt ENISA om de volgende stappen te ondernemen:

- samen met de desbetreffende nationale bevoegde instanties, betrokken belanghebbende partijen, internationale en Europese normalisatieorganisaties en het Gemeenschappelijk Centrum voor Onderzoek van de Europese Commissie **technische richtsnoeren en aanbevelingen te ontwikkelen voor de vaststellingen van normen en goede praktijken op het gebied van NIB** in de publieke en private sector.

De Commissie verzoekt publieke en private belanghebbende partijen de volgende stappen te ondernemen:

- de ontwikkeling en vaststelling van door de branche opgestelde **beveiligingsnormen**, technische normen en beginselen "security-by-design" en "privacy-by-design" door fabrikanten van ICT-producten en dienstverleners, met

[28] Met name in het kader van de norm M/490 inzake intelligente netwerken met betrekking tot de eerste reeks normen die zijn gericht op een intelligente netwerk- en referentiearchitectuur.

inbegrip van cloud providers. Nieuwe generaties software en hardware dienen te beschikken over **sterkere geïntegreerde en gebruiksvriendelijke beveiligingskenmerken**;

- door de branche opgestelde normen voor de prestaties van bedrijven op het gebied van cyberbeveiliging ontwikkelen en de voor het publiek beschikbare informatie verbeteren door **beveiligingslabels** of keurmerken te ontwikkelen, waarmee de consument zich beter op de markt kan oriënteren.

Investeringen in onderzoek en ontwikkeling alsmede innovatie stimuleren

Onderzoek en ontwikkeling kunnen een steunpilaar zijn voor een sterk industriebeleid, een betrouwbare Europese ICT-industrie bevorderen, een impuls geven aan de interne markt en Europa minder afhankelijk maken van uitheemse technologieën. Met onderzoek en ontwikkeling kunnen de technologische lacunes op het gebied van ICT-beveiliging worden gevuld, voorbereidingen worden getroffen voor de volgende generatie uitdagingen op beveiligingsgebied, worden ingegaan op de permanente evolutie van de behoeften van de gebruikers en kunnen de voordelen van technologie voor tweeërlei gebruik ten volle worden benut. Bovendien dient de ontwikkeling van de cryptografie permanent te worden ondersteund. Als aanvulling daarop dienen te worden nagestreefd de resultaten van onderzoek en ontwikkeling om te zetten in commerciële oplossingen door de nodige prikkels te bieden en de passende beleidsvoorwaarden te scheppen.

De EU dient Horizon 2020[29], het kaderprogramma voor onderzoek en innovatie dat in 2014 van start gaat, optimaal te benutten. Het voorstel van de Commissie omvat specifieke doelstellingen voor betrouwbare ICT alsmede voor de bestrijding van cybercriminaliteit, die in overeenstemming met deze strategie zijn. Met Horizon 2020 wordt beveiligingsonderzoek op het gebied van opkomende ICT-technologieën ondersteund; worden oplossingen voorzien voor volledig beveiligde ICT-systemen, -diensten en -toepassingen; worden prikkels gegeven voor de implementatie en vaststelling van bestaande oplossingen; en wordt de interoperabiliteit van netwerk- en informatiesystemen bevorderd. Op EU-niveau zal er in het bijzonder aandacht worden besteed aan de optimalisatie en betere coördinatie van de diverse financieringsprogramma's (Horizon 2020, het fonds voor interne veiligheid en EDA-onderzoek met inbegrip van het Europese samenwerkingskader).

De Commissie zal de volgende stappen ondernemen:

- in het kader van Horizon 2020 maatregelen op het gebied van ICT nemen wat de persoonlijke levenssfeer en de veiligheid betreft, variërend van onderzoek en ontwikkeling tot innovatie en toepassing. *Daarnaast in het kader van Horizon 2020 werktuigen en instrumenten ontwikkelen om criminele en terroristische activiteiten te bestrijden die op cyberspace zijn gericht;*
- mechanismen opzetten voor betere coördinatie van het onderzoeksbeleid van de EU-instellingen en de lidstaten alsmede de lidstaten aanmoedigen om meer in onderzoek en ontwikkeling te investeren.

[29] Horizon 2020 is het financiële instrument voor de tenuitvoerlegging van de , een -vlaggenschipinitiatief dat het Europese concurrentievermogen mondiaal veilig moet stellen. Het nieuwe kaderprogramma voor onderzoek en innovatie van de EU loopt van 2014 tot en met 2020 en is onderdeel van de inspanningen om in Europa nieuwe groei en banen te creëren.

De Commissie verzoekt de lidstaten om:

- uiterlijk eind 2013 goede praktijken te onwikkelen voor het gebruik van het **grote investeringsvolume van overheidsinstanties** (bijvoorbeeld door middel van openbare aanbestedingen) om de ontwikkeling en toepassing van beveiligingskenmerken in ICT-producten en -diensten te bevorderen;
- aan te moedigen dat de sector en de academische wereld in een vroeg stadium worden betrokken bij het ontwikkelen en coördineren van oplossingen. Hierbij dienen de industriële basis van Europa en aanverwante, door onderzoek en ontwikkeling geproduceerde, technologische innovaties optimaal te worden benut en dient het onderzoeksbeleid van civiele organisaties en dat van militaire organisaties op elkaar te worden afgestemd.

De Commissie vraagt Europol en ENISA om de volgende stappen te ondernemen:

- nieuwe trends en behoeften met betrekking tot ontwikkelingen op het gebied van patronen in de cybercriminaliteit en -beveiliging in het oog te houden, zodat op basis daarvan adequate digitale forensische instrumenten en technologieën kunnen worden ontwikkeld.

De Commissie verzoekt publieke en private belanghebbende partijen de volgende stappen te ondernemen:

- samen met de verzekeringssector **geharmoniseerde berekeningsmethoden voor risicopremies** te ontwikkelen, waardoor bedrijven die in beveiliging hebben geïnvesteerd, kunnen profiteren van lagere risicopremies.

2.5. Een coherent internationaal cyberbeveiligingsbeleid voor de Europese Unie ontwikkelen en de kernwaarden van de EU uitdragen

Het behouden van een open, vrije en beveiligde cyberspace is een wereldwijde uitdaging die de EU samen met de desbetreffende internationale partners en organisaties, de private sector en het maatschappelijk middenveld dient aan te gaan.

De EU wil met haar internationale cyberspacebeleid openheid en vrijheid op internet bevorderen, de ontwikkeling van gedragsnormen aanmoedigen en bestaande internationale wetgeving in cyberspace toepassen. Verder zal de EU maatregelen ondernemen om de digitale kloof te dichten en actief deelnemen aan internationale inspanningen om capaciteit op het gebied van cyberveiligheid op te bouwen. Bij het internationale engagement van de EU met betrekking tot cyberkwesties gaat zij uit van de kernwaarden van de EU, namelijk de menselijke waardigheid, vrijheid, democratie, gelijkheid, de rechtsstaat en de eerbiediging van de grondrechten.

Integratie van cyberspacekwesties in de externe betrekkingen van de EU en het gemeenschappelijk buitenlands en veiligheidsbeleid

De Commissie, de hoge vertegenwoordiger en de lidstaten dienen een samenhangend internationaal EU-beleid inzake cyberspace te formuleren dat gericht is op een sterker engagement en intensievere relaties met de voornaamste internationale partners en organisaties alsmede met het maatschappelijk middenveld en de private sector. EU-raadplegingen met internationale partners over cyberkwesties dienen zodanig te zijn ontworpen, gecoördineerd en uitgevoerd dat er een meerwaarde wordt toegevoegd aan

bestaande bilaterale dialogen tussen de EU-lidstaten en derde landen. De EU zal eens te meer de nadruk leggen op de dialoog met derde landen en zich met name richten op gelijkgestemde partners die de EU-waarden onderschrijven. Zij zal het streven naar een hoog niveau van gegevensbescherming, onder meer bij de overdracht van persoonsgegevens naar derde landen. Om de wereldwijde uitdagingen in cyberspace aan te pakken, zal de EU streven naar nauwere samenwerking met organisaties die op dit gebied actief zijn, zoals de Raad van Europa, de OESO, de VN, de OVSE, de NAVO, de AU, de ASEAN en de OAS. Op bilateraal niveau is samenwerking met de Verenigde Staten bijzonder belangrijk. Deze samenwerking zal verder worden verdiept, met name in het kader van de EU/VS-werkgroep inzake cyberbeveiliging en cybercriminaliteit.

Een van de belangrijkste elementen van het internationale cyberbeleid van de EU is het bevorderen van cyberspace als ruimte van vrijheid en grondrechten. Het uitbreiden van de toegang tot het internet werkt wereldwijd democratische hervormingen in de hand. De wereldwijde toename van connectiviteit mag niet vergezeld gaan van censuur of grootschalige bewaking. De EU dient maatschappelijk verantwoord ondernemen te bevorderen[30] en internationale initiatieven op te zetten om het wereldwijde overleg op dit gebied te bevorderen.

De verantwoordelijkheid voor een veiligere cyberspace ligt bij iedereeen die is betrokken bij de wereldwijde informatiemaatschappij, uiteenlopend van de burgers tot overheden. De EU steunt inspanningen om gedragsnormen voor cyberspace te formuleren, waaraan alle belanghebbende partijen zich dienen te houden. De EU verwacht van burgers dat zij hun burgerplichten, sociale verantwoordelijkheden en de wet nakomen, maar ook staten dienen zich aan normen en bestaande wetgeving te houden. Met betrekking tot de internationale veiligheid moedigt de EU de ontwikkeling van maatregelen aan die het vertrouwen in cyberbeveiliging vergroten, waardoor de transparantie toeneemt en het gedrag van de staat minder snel verkeerd wordt geïnterpreteerd.

De EU is niet van mening dat er nieuwe internationale rechtsinstrumenten inzake cyberkwesties nodig zijn.

De wettelijke verplichtingen van het Internationaal Verdrag inzake burgerrechten en politieke rechten, het Europees Verdrag voor de rechten van de mens en het EU-Handvest van de grondrechten dienen ook op internet te worden nagekomen. De EU zal zich erop richten te waarborgen dat deze maatregelen ook in cyberspace worden gehandhaafd.

Met betrekking tot de bestrijding van cybercriminaliteit is het Verdrag van Boedapest een instrument dat derde landen kunnen vaststellen. Het biedt een model voor het opstellen van nationale wetgeving inzake cybercriminaliteit en een basis voor internationale samenwerking op dit gebied.

Als gewapende conflicten ook in cyberspace worden uitgevochten, is internationaal humanitair recht en eventueel de wetgeving inzake mensenrechten van toepassing.

Ontwikkeling van capaciteit op het gebied van cyberbeveiliging en veerkrachtige informatie-infrastructuur in derde landen

De soepele werking van de infrastructuur die ten grondslag ligt aan communicatiediensten en deze mogelijk maakt, heeft baat bij intensievere internationale samenwerking. Hieronder

[30] Een vernieuwde EU-strategie 2011-2014 ter bevordering van maatschappelijk verantwoord ondernemen; COM(2011) 681 definitief.

vallen onder meer het uitwisselen van beste praktijken, informatie en vroegtijdige waarschuwingen alsmede gezamenlijke oefeningen met betrekking tot het beheer van incidenten. De EU zal aan deze doelstelling bijdragen door haar huidige inspanningen ter versterking van internationale samenwerkingsverbanden op het gebied van bescherming van kritieke informatie-infrastructuur (CIIP), waarbij overheden en de private sector zijn betrokken, te intensiveren.

Door een gebrek aan open, veilige en interoperabele toegang kunnen niet alle delen van de wereld profiteren van de positieve effecten van internet. De Europese Unie zal de betrokken landen daarom blijven steunen bij de ontwikkeling van de toegang en het gebruik van internet voor hun inwoners, bij de waarborging van de integriteit en veiligheid van internet en de doeltreffend bestrijding van cybercriminaliteit.

De Commissie en de hoge vertegenwoordiger zullen samen met de lidstaten de volgende maatregelen nemen:

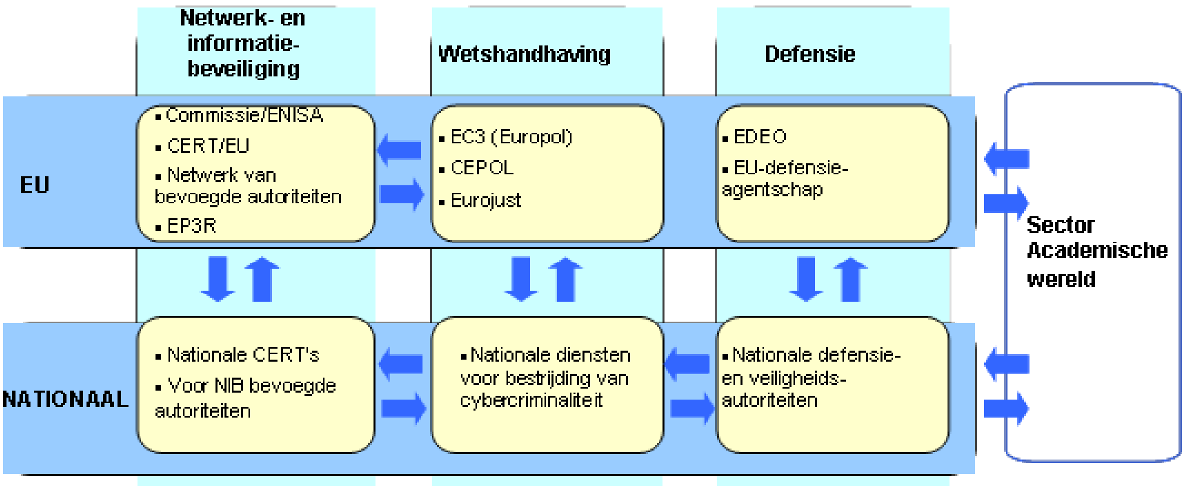
- streven naar een samenhangend internationaal cyberspacebeleid van de EU om ervoor te zorgen dat het engagement van de voornaamste internationale partners en organisaties toeneemt, cyberkwesties in het GBVB worden geïntegreerd en de coördinatie inzake wereldwijde cyberkwesties wordt verbeterd;
- steunen van de ontwikkeling van gedragsnormen en maatregelen die het vertrouwen in cyberbeveiliging vergroten. Faciliteren van dialogen over mogelijkheden om bestaande internationale wetgeving in cyberspace en het Verdrag van Boedapest toe te passen om cybercriminaliteit te bestrijden;
- bevorderen en beschermen van de grondrechten, met inbegrip van de toegang tot informatie en vrijheid van meningsuiting, met de nadruk op: a) het ontwikkelen van nieuwe openbare richtsnoeren inzake vrijheid van meningsuiting op digitaal gebied en daarbuiten; b) toezicht houden op de uitvoer van producten of diensten die voor digitale censuur of grootschalige bewaking kunnen worden gebruikt; c) ontwikkelen van maatregelen en instrumenten om de toegang tot alsmede de openheid en veerkracht van het internet uit te breiden om censuur of grootschalige bewaking door middel van communicatietechnologie tegen te gaan; d) de belanghebbende partijen aanmoedigen en de mogelijkheid bieden communicatietechnologie te gebruiken om grondrechten te bevorderen;
- overleggen met internationale partners en organisaties, de private sector en het maatschappelijk middenveld om de opbouw van capaciteit in derde landen over de hele wereld te steunen, toegang tot informatie en open internet te verbeteren, cyberdreigingen te voorkomen en bestrijden, met inbegrip van toevallige gebeurtenissen, cybercriminaliteit en cyberterrorisme alsmede donorcoördinatie te ontwikkelen voor het aansturen van inspanningen om capaciteit op te bouwen;
- gebruikmaken van diverse EU-hulpinstrumenten voor het opbouwen van capaciteit op het gebied van cyberbeveiliging, met inbegrip van bijstand voor de opleiding van rechtshandhavings-, justitieel en technisch personeel met betrekking tot de bestrijding van cyberdreigingen; steun geven aan nieuw nationaal beleid alsmede nieuwe strategieën en instanties op dit gebied in

derde landen; • verbeteren van de beleidscoördinatie en de informatie-uitwisseling door middel van internationale netwerken in het kader van de bescherming van kritieke informatie-infrastructuur, zoals het Meridian-proces, samenwerking tussen de voor NIB bevoegde nationale instanties en overige betrokkenen.

3. TAKEN EN VERANTWOORDELIJKHEDEN

De digitale economie en samenleving kennen talloze verbindingen, waardoor cyberincidenten niet door grenzen worden tegengehouden. Alle betrokkenen, met inbegrip van de voor NIB bevoegde instanties, CERT's en wetshandhavingsinstanties en de sector, dienen zowel nationaal als op EU-niveau de verantwoordelijkheid op zich te nemen cyberbeveiliging te versterken. Aangezien er diverse rechtskaders en jurisdicties van toepassing kunnen zijn, is het van groot belang dat de EU de taken en verantwoordelijken van de talrijke betrokkenen verduidelijkt.

Gezien de complexiteit van dit probleem en de grote verscheidenheid van de betrokkenen, is gecentraliseerd Europees toezicht geen oplossing. De nationale overheden zijn het geschiktst om de preventie en bestrijding van cyberincidenten te organiseren en om contact te legen de met private sector en het publiek en daarbij rekening te houden met hun vastgelegde beleidslijnen en rechtskaders. Het is mogelijk dat de gevaren grensoverschrijdend zijn, of deze zijn dat in de praktijk al. Daarom zijn er voor een doeltreffende nationale reactie vaak ook maatregelen op EU-niveau nodig. Om cyberbeveiliging op een grondige manier aan te pakken, dienen de activiteiten drie belangrijke gebieden te beslaan – netwerk- en informatiebeveiliging, wetshandhaving en defensie – die onder verschillende rechtskaders vallen:



3.1. Overleg tussen de voor NIB bevoegde instanties/CERT's, de wetshandhavingsinstanties en defensie

Nationaal niveau

De lidstaten dienen (nu al of anders naar aanleiding van deze strategie) te beschikken over structuren met betrekking tot de veerkracht van cyberspace, cybercriminaliteit en cyberdefensie. Verder dienen zij voldoende capaciteit op te bouwen om cyberincidenten aan te pakken. Voor optimale coördinatie op nationaal niveau dienen alle betrokken ministeries

samen te werken, aangezien het mogelijk is dat een aantal verschillende instanties operationeel verantwoordelijk zijn voor bepaalde aspecten op het gebied van cyberbeveiliging en het van belang is dat de private sector erbij wordt betrokken. De lidstaten dienen in hun nationale strategieën inzake cyberbeveiliging de taken en verantwoordelijkheden van de diverse nationale instanties vast te leggen.

Uitwisseling van informatie tussen de nationale instanties en de private sector dient te worden aangemoedigd om ervoor te zorgen dat de lidstaten en de private sector een goed overzicht hebben over de verschillende dreigingen en goed op de hoogte zijn van nieuwe trends en technieken die enerzijds worden toegepast om cyberaanvallen uit te voeren en anderzijds om er sneller op te reageren. Door nationale samenwerkingsplannen inzake NIB vast te leggen die worden toegepast in geval van cyberincidenten, zijn de lidstaten in staat om taken en verantwoordelijken duidelijk toe te wijzen en om de bestrijding te optimaliseren.

EU-niveau

Net als op nationaal niveau gaan er op EU-niveau diverse instanties over cyberbeveiliging. ENISA, Europol/EC3 en EDA zijn drie agentschappen die respectievelijk actief zijn op de gebieden NIB, wetshandhaving en defensie. Elk agentschap heeft een raad bestuur waarin de lidstaten vertegenwoordigd zijn en biedt een platform voor coördinatie op EU-niveau.

Coördinatie en samenwerking tussen ENISA, Europol/EC3 en EDA op de gebieden waarop zij gezamenlijk actief zijn, wordt aangemoedigd, met name met betrekking tot de analyse van trends en gevaren, opleidingen en uitwisseling van beste praktijken. Zij dienen samen te werken en tegelijkertijd hun specifieke eigenschappen te behouden. Deze agentschappen dienen samen met CERT-EU, de Commissie en de lidstaten de ontwikkeling van een hechte gemeenschap van technische en beleidsdeskundigen op dit gebied te ondersteunen.

Informele kanalen voor de coördinatie en samenwerking zullen worden aangevuld met meer structurele verbindingen. Militaire staf van de EU en het cyberdefensieteam van EDA kunnen de coördinatie op defensiegebied op zich nemen. De programmaraad van Europol/EC3 dient als platform voor overleg tussen onder meer EUROJUST, CEPOL, de lidstaten[31], ENISA en de Commissie, waar zij hun specifieke expertise kunnen uitwisselen en kunnen waarborgen dat EC3 bij haar maatregelen gericht is op partnerschap; alle belanghebbende partijen kunnen hierbij hun expertise inbrengen en hun mandaten worden geëerbiedigd. Op basis van het nieuwe mandaat van ENISA kunnen de banden met Europol en de belanghebbende partijen uit de sector worden versterkt. Maar bovenal wordt er door het wetgevingsvoorstel inzake NIB van de Commissie een samenwerkingskader geschapen door middel van een netwerk van nationale instanties die voor NIB bevoegd zijn en wordt de uitwisseling van informatie tussen deze instanties en wetshandhavingsinstanties bevorderd.

Internationaal niveau

De Commissie en de hoge vertegenwoordiger waarborgen samen met de lidstaten gecoördineerde internationale maatregelen op het gebied van cyberbeveiliging. Daarbij bevestigen de Commissie en de hoge vertegenwoordiger EU-kernwaarden en bevorderen zij een vreedzaam, open en transparant gebruik van cybertechnologieën. De Commissie, de hoge vertegenwoordiger en de lidstaten voeren een beleidsdialoog met internationale partners en internationale organisaties als de Raad van Europa, de OESO, de OVSE, de NAVO en de VN.

[31] Via hun vertegenwoordiging in de EU-taskforce cybercriminaliteit, die bestaat uit de leiders van de EU-cybercriminaliteitseenheden van de lidstaten.

3.2. EU-steun bij een cyberincident of -aanval van ernstige aard

Ernstige cyberincidenten- of aanvallen hebben waarschijnlijk een impact op overheden, bedrijven en burgers in de EU. Door deze strategie en met name door de voorgestelde richtlijn inzake netwerk- en informatiebeveiliging wordt de preventie, opsporingen en bestrijding van cyberincidenten verbeterd en houden de lidstaten en de Commissie elkaar beter op de hoogte over ernstige cyberincidenten- of aanvallen. Welk bestrijdingsmechanisme er wordt toegepast, hangt echter af van de aard, omvang en grensoverschrijdende gevolgen van het incident.

Als het incident een aanzienlijke impact heeft op de bedrijfscontinuïteit, voorziet de richtlijn inzake netwerk- en informatiebeveiliging erin dat er nationale samenwerkingsplannen voor NIB of soortgelijke plannen van de Unie in werking worden gesteld, afhankelijk van de mate waarin het incident grensoverschrijdende gevolgen heeft. In dergelijke gevallen wordt er informatie uitgewisseld en steun verleend via het netwerk van instanties die voor NIB bevoegd zijn. Hierdoor kunnen de getroffen netwerken en diensten in stand gehouden en/of hersteld worden.

Als er bij het incident sprake is van een strafbaar feit, dient Europol/EC3 te worden ingelicht, zodat deze instantie samen met de wetshandhavingsinstanties uit de desbetreffende landen een onderzoek kan instellen, bewijsmateriaal kan verzamelen, de daders kan identificeren en ervoor kan zorgen dat zij uiteindelijk worden vervolgd.

Als er bij het incident waarschijnlijk sprake is van cyberspionage of een door een staat gesteunde aanval, of als het incident gevolgen heeft voor de nationale veiligheid, lichten de nationale veiligheids- en defensie-instanties de desbetreffende tegenhangers in, zodat deze weten dat zij worden aangevallen en zij zich kunnen verdedigen. Er worden dan mechanismen voor vroegtijdige waarschuwingen en indien nodig crisismanagement of andere procedures in werking gesteld. Een cyberincident of -aanval van bijzonder ernstige aard kan voldoende reden zijn voor een lidstaat om een beroep te doen op de solidariteitsclausule van de EU (artikel 222 van het Verdrag betreffende de werking van de Europese Unie).

Als er bij het incident waarschijnlijk persoonsgegevens in gevaar zijn gebracht, dienen op grond van Richtlijn 2002/58/EG de nationale gegevensbeschermingsautoriteiten of de nationale toezichthoudende instanties te worden ingelicht.

De aanpak van cyberincidenten en -aanvallen heeft tot slot baat bij contactnetwerken en steun van internationale partners. Hieronder vallen onder meer technische maatregelen die de gevolgen inperken, strafrechtelijk onderzoek of de toepassing van bestrijdingsmechanismen in het kader van crisismanagement.

4. CONCLUSIES EN FOLLOW-UP

De voorgestelde strategie inzake cyberbeveiliging van de Europese Unie, die is uitgestippeld door de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid, schetst de visie die de EU op dit gebied heeft en omvat de vereiste maatregelen, op basis van een sterke bescherming en bevordering van de rechten van de burgers, om de digitale omgeving in de EU de veiligste in de wereld te maken[32].

---

[32] De financiering van de strategie valt binnen de bedragen die zijn uitgetrokken voor elk van de desbetreffende beleidsterreinen (CEF, Horizon 2020, het fonds voor interne veiligheid, GBVB en externe samenwerking, met name het stabiliteitsinstrument), zoals vastgelegd in het voorstel van de Commissie voor het meerjarig financieel kader 2014-2020 (afhankelijk van de goedkeuring van de

Deze visie kan alleen in de praktijk worden gebracht op basis van een daadwerkelijke partnerschap tussen alle betrokkenen, waarbij allen verantwoordelijkheid op zich nemen en de desbetreffende uitdagingen aanpakken.

De Commissie en de hoge vertegenwoordiger vragen de Raad en het Europees Parlement daarom hun goedkeuring aan de strategie te hechten en hun bijdrage te leveren om de beschreven maatregelen te laten slagen. Aanzienlijke steun en betrokkenheid van de private sector en het maatschappelijk middenveld zijn eveneens onontbeerlijk, aangezien zij van groot belang zijn voor het verhogen van ons beveiligingsniveau en het waarborgen van de burgerrechten.

Het is nu tijd om actie te ondernemen. De Commissie en de hoge vertegenwoordiger zijn vastbesloten om met alle betrokkenen samen te werken, zodat Europa de beveiliging krijgt die het nodig heeft. Om ervoor te zorgen dat de strategie spoedig ten uitvoer wordt gelegd en ten aanzien van eventuele ontwikkelingen wordt geëvalueerd, zullen zij alle relevante partijen uitnodigen voor een conferentie op hoog niveau en over twaalf maanden beoordelen welke vooruitgang er is geboekt.

begrotingsautoriteit en de bedragen die uiteindelijk in het meerjarig financieel kader voor 2014-2020 worden vastgesteld). Met betrekking tot de noodzaak om overeenstemming te bereiken met het aantal beschikbare posten voor de gedecentraliseerde agentschappen en het submaximum voor gedecentraliseerde agentschappen in elke uitgavenrubriek in het volgende meerjarig financieel kader, worden de agentschappen (CEPOL, EDA ENISA, EUROJUST en EUROPOL/EC3) die op grond van deze mededeling worden verzocht nieuwe taken op zich te nemen, aangemoedigd dit te doen voor zover het daadwerkelijke vermogen van het agentschap om meer middelen te absorberen is vastgesteld en alle mogelijkheden voor herindeling zijn bepaald.